PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : G06F 12/14, 1/00 — A1

(11) International Publication Number: WO 94/01821

(43) International Publication Date: 20 January 1994 (20.01.94)

(21) International Application Number: PCT/US93/06511

(22) International Filing Date: 9 July 1993 (09.07.93)

(30) Priority data:
07/911,900 10 July 1992 (10.07.92) US

(71) Applicant: SECURE COMPUTING CORPORATION [US/US]; 2675 Long Lake Road, Roseville, MN 55113-2536 (US).

(72) Inventors: BOEBERT, William, E. ; 4915 DuPont Avenue South, Minneapolis, MN 55409 (US). HANSON, Mark, H. ; 3560 Baltic Avenue, Eagan, MN 55122 (US). MARKHAM, Thomas, R. ; 709 River Lane, Anoka, MN 55303 (US).

(74) Agent: BRUESS, Steven, C.; Merchant, Gould, Smith, Edell, Welter & Schmidt, 3100 Norwest Center, 90 South Seventh Street, Minneapolis, MN 55402 (US).

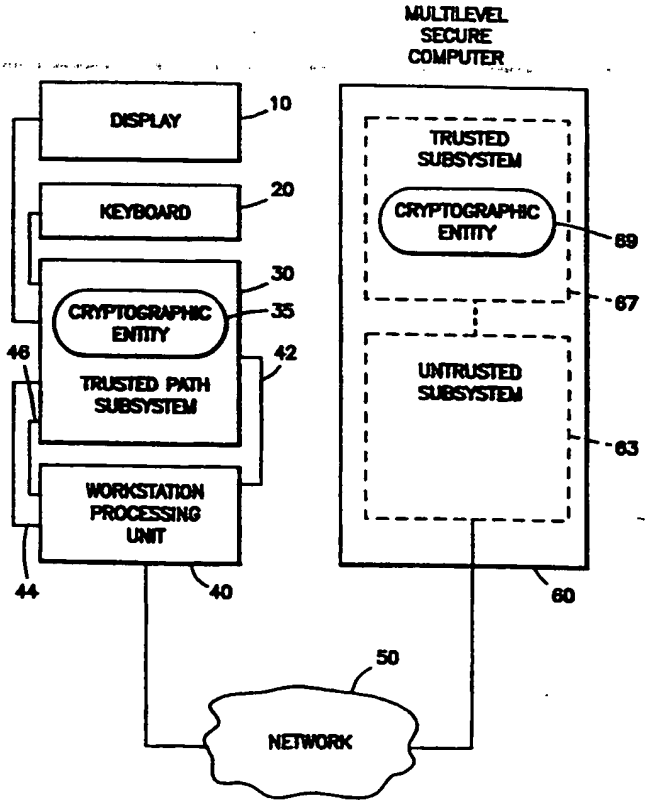
(81) Designated States: AT, AU, BB, BG, BR, BY, CA, CH, CZ, DE, DK, ES, FI, GB, HU, JP, KP, KR, KZ, LK, LU, MG, MN, MW, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SK, UA, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: TRUSTED PATH SUBSYSTEM FOR WORKSTATIONS

(57) Abstract

A method and apparatus for ensuring secure communication over an unsecured communications medium between a user working on an unsecured workstation or computer and a host computer. A secure user interface is created by inserting a trusted path subsystem between input/output devices to the workstation and the workstation itself. Data transferred from the input/output devices is intercepted, encrypted and transmitted in packets to the host computer. Packets of screen display data from the host computer are decrypted and presented within a user-defined screen overlay.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**FR**	France	**MR**	Mauritania
AU	Australia	**GA**	Gabon	**MW**	Malawi
BB	Barbados	**GB**	United Kingdom	**NE**	Niger
BE	Belgium	**GN**	Guinea	**NL**	Netherlands
BF	Burkina Faso	**GR**	Greece	**NO**	Norway
BG	Bulgaria	**HU**	Hungary	**NZ**	New Zealand
BJ	Benin	**IE**	Ireland	**PL**	Poland
BR	Brazil	**IT**	Italy	**PT**	Portugal
BY	Belarus	**JP**	Japan	**RO**	Romania
CA	Canada	**KP**	Democratic People's Republic of Korea	**RU**	Russian Federation
CF	Central African Republic			**SD**	Sudan
CG	Congo	**KR**	Republic of Korea	**SE**	Sweden
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovak Republic
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LU**	Luxembourg	**TD**	Chad
CS	Czechoslovakia	**LV**	Latvia	**TG**	Togo
CZ	Czech Republic	**MC**	Monaco	**UA**	Ukraine
DE	Germany	**MG**	Madagascar	**US**	United States of America
DK	Denmark	**ML**	Mali	**UZ**	Uzbekistan
ES	Spain	**MN**	Mongolia	**VN**	Viet Nam
FI	Finland				

TRUSTED PATH SUBSYSTEM FOR WORKSTATIONS

Background of the Invention

Field of the Invention

The present invention relates to an apparatus and method for providing a trusted computer system based on untrusted computers, and more particularly to an apparatus and method for providing a trusted path mechanism between a user node based on an untrusted computer or workstation and a trusted subsystem.

Background Information

Advances in computer and communications technology have increased the free flow of information within networked computer systems. While a boon to many, such a free flow of information can be disastrous to those systems which process sensitive or classified information. In response to this threat, trusted computing systems have been proposed for limiting access to classified information to those who have a sufficient level of clearance. Such systems depend on identifying the user, authenticating (through password, biometrics, etc.) the user's identity and limiting that user's access to files to those files over which he or she has access rights. In addition, a trusted path mechanism is provided which guarantees that a communication path established between the Trusted Computer Base (TCB) and the user cannot be emulated or listened to by malicious hardware or software. Such a system is described in U.S. Patent Nos. 4,621,321; 4,713,753; and 4,701,840 granted to Boebert et al. and assigned to the present assignee, the entire disclosures of which are hereby incorporated by reference.

The last decade has marked a shift in the distributing of computational resources. Instead of connecting a large number of relatively "dumb" terminals to a mainframe computer, the automatic data processing

environment has gradually shifted to where a large number of current systems are file server systems. In a file server system, relatively low cost computers are placed at each user's desk while printers and high capacity data storage devices are located near the server or servers. Files stored in the high capacity data storage devices are transferred to the user's computer for processing and then either saved in local storage or transferred back to the storage devices. Documents to be printed are transferred as files to a print server; the print server then manages the printing of the document.

An even more loosely coupled distributed computing approach is based on the client-server paradigm. Under the client-server paradigm, one or more client processes operating on a user's workstation gain access to one or more server processes operating on the network. As in file server systems, the client processes handle the user interface while the server processes handle storage and printing of files. In contrast with file server systems, however, the client processes and the server processes share data processing responsibilities. A more complete discussion of distributed computing is contained in "Client-Server Computing" by Alok Sinha, published in the July 1992 issue of *Communications of the ACM*.

Both the file server and the client-server paradigms depend heavily upon the availability of low-cost computer systems which can be placed at each user's desk. The low-cost systems are then connected through a network such as a LAN or a WAN to the server systems. Such a networked system is illustrated in the block diagram shown in Fig. 1.

In Fig. 1, a workstation processing unit 40 is connected through a network 50 to a host computer 60. Workstation unit 40 is also connected through video port

44 and keyboard port 46 to display unit 10 and keyboard 20, respectively.

In a typical distributed computer system, the workstations 40, the host computers 60 and the connecting networks 50 are all at great risk of a security breach. Trusted computer systems based on host computers such as the Multilevel Secure (MLS) Computer 60 shown in Fig. 1 make security breaches at the host computer more difficult by partitioning the system to isolate security critical (trusted) subsystems from nonsecurity critical (untrusted) subsystems. Such computers do little, however, to prevent security breaches on network 50 or at user workstation 40.

A Multi-Level Secure (MLS) Computer such as is shown in Fig. 1 is capable of recognizing data of varying sensitivity and users of varying authorizations and ensuring that users gain access to only that data to which they are authorized. For example, an MLS computer can recognize the difference between company proprietary and public data. It can also distinguish between users who are company employees and those who are customers. The MLS computer can therefore be used to ensure that company proprietary data is available only to users who are company employees.

Designers of MLS computers assume that unauthorized individuals will use a variety of means, such as malicious code and active and passive wiretaps, to circumvent its controls. The trusted subsystem of an MLS computer must therefore be designed to withstand malicious software executing on the untrusted subsystem, to confine the actions of malicious software and render them harmless. One mechanism for avoiding malicious software is to invoke a trusted path, a secure communications path between the user and the trusted subsystem. A properly designed trusted path ensures that information viewed or sent to the trusted subsystem is not copied or modified along the way.

Extension of the trusted path through the network to the user is, however, difficult. As is described in a previously filed, commonly owned U.S. patent application entitled "Secure Computer Interface" (U.S. Patent Application No. 07/676,885 filed March 28, 1991 by William E. Boebert), "active" and "passive" network attacks can be used to breach network security. Active attacks are those in which masquerading "imposter" hardware or software is inserted into the network communications link. For example, hardware might be inserted that emulates a user with extensive access privileges in order to access sensitive information. "Passive" network attacks include those in which a device listens to data on the link, copies that data and sends it to another user. A system for ensuring secure data communications over an unsecured network is described in the above-identified patent application. That application is hereby incorporated by reference.

Active and passive attacks can also be used to breach computer security through software running on an untrusted user computer, an untrusted host or in the untrusted subsystem of a Multilevel Secure Computer. For example, malicious software running in the workstation could present itself to an authorized user as the trusted subsystem, and cause that user to enter highly sensitive data, such as a password. The data is then captured and given to the attacker. Under a passive software attack, data which is intended for one user could be copied and sent to a user who is not authorized to work with it.

Systems for ensuring secure communications over an unsecured network have been limited to date to scrambling devices which encrypt data written to the network and decrypt data received from the network. Such systems are limited in that they provide no assurance that the user's computer is secure or that the user has, in fact, established a trusted path to the

trusted subsystem. Therefore, despite the fact that the communications link is secure, it is possible for a user on the computer to be misled into believing that a program executing on his computer is actually running on the host computer.

What is needed is a mechanism for extending the trusted path from the trusted subsystem of the host computer to the user of an untrusted computer or workstation. Such a method should provide access to the workstation for normal workstation activities while shielding confidential data so that it cannot be read by software executing on the unsecured workstation.

Summary of the Invention

The present invention provides a method and apparatus for ensuring secure communication over an unsecured communications medium between a user working on an unsecured workstation or computer and a host computer. A secure user interface is created by inserting a trusted path subsystem between input/output devices to the workstation and the workstation itself. Data transferred from the input/output devices is intercepted, encrypted and transmitted in packets to the host computer. Packets of screen display data from the host computer are decrypted and presented within a user-defined screen overlay.

According to another aspect of the present invention, a method is disclosed for ensuring secure file transfers between an unsecured workstation and a host computer. A file to be transferred is downloaded to a trusted path subsystem inserted between the workstation and its keyboard and display device. The trusted path subsystem presents a representation of the file on the display device where the user can verify that the file is as expected. The verified file is then encrypted and transferred as packets to the host computer.

Brief Description of the Drawings

FIG. 1 is a system level block diagram representation of a networked computer system.

FIG. 2 is a system level block diagram representation of a secure networked computer system according to the present invention.

FIG. 3 is a block diagram representation of a user node including a trusted path subsystem according to the present invention.

FIG. 4 is a block diagram representation of a user node including a different embodiment of a trusted path subsystem according to the present invention.

FIG. 5 is an electrical block diagram representation of one embodiment of the trusted path subsystem according to the present invention.

FIG. 6 is a representation of a secure window overlay according to the present invention.

Detailed Description of the Preferred Embodiments

In the following Detailed Description of the Preferred Embodiments, reference is made to the accompanying Drawings which form a part hereof, and in which are shown by way of illustration specific embodiments in which the invention may be practiced. It is to be understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

The present invention provides a method and apparatus for ensuring secure communication over an unsecured communications medium between a user working on an unsecured workstation or computer and a host

computer. A secure user interface is created by inserting a trusted path subsystem between input/output devices to the workstation and the workstation itself. Data transferred from the input/output devices is intercepted, encrypted and transmitted in packets through the workstation to the host computer. Packets of screen display data from the host computer are decrypted and presented within a user-defined screen overlay.

Cryptographic entities in the trusted path subsystem and the host computer apply end-to-end encryption to confidential data transferred to and from the network. End-to-end encryption is a technique whereby data is encrypted as close to its source as possible and decrypted only at its ultimate destination. This technique differs from link encryption, in which data is decrypted, then encrypted again as it moves from the sender to the receiver.

The present invention extends the notion of end-to-end encryption by performing the encryption/decryption closer to the originator and receiver than prior systems. In the present invention, the encryption/decryption is performed as the data enters and leaves the input/output device. The data is therefore protected from malicious software which might be operating on the workstation and from active or passive attacks on the network.

A secure networked computer system constructed according to the present invention is illustrated generally in Fig. 2. In Fig. 2, a workstation processing unit 40 is connected through a network 50 to a host computer 60. Workstation 40 can be any computer, workstation or X terminal which has a separate data path for communication between a trusted path subsystem 30 and the workstation. For instance, workstation 40 can be a commercially available workstation such as the UNIX workstations manufactured by Sun Microsystems, Mountain

View, California, an IBM PC compatible such as those available from Compaq, Houston, Texas or an X terminal such as Model NCD19g from Network Computing Devices, Inc, Mountain View, California.

Trusted path subsystem 30 is connected to workstation 40 (through auxiliary data port 42), keyboard 20 and display 10. Trusted path subsystem 30 includes cryptographic entity 35 for encrypting and decrypting information transferred between display 10, keyboard 20 and workstation 40.

Host computer 60 is a Multi-Level Secure computer which includes a trusted subsystem 67 and an untrusted subsystem 63. Trusted subsystem 67 includes a cryptographic entity 69 for encrypting and decrypting data transferred between trusted subsystem 67, untrusted subsystem 63, and network 50. In another embodiment of the present invention, host computer 60 is a computer running a trusted subsystem software package. In that embodiment, cryptographic entity 69 would be implemented in software.

In the embodiment shown in Fig. 2, all communication between trusted path subsystem 30 and host computer 60 is done via workstation 40. In one such embodiment, auxiliary data port 42 is an RS-232 line connecting workstation 40 and subsystem 30. Communications software running on workstation 40 receives encrypted packets from the trusted path subsystem and sends them to the host computer. In a like manner, encrypted packets from host computer 60 are received by workstation 40 and transferred to subsystem 30 for decrypting. This type of interface is advantageous since a standard communications protocol can be defined for transfers between subsystem 30 and host computer 60. Workstation 40 then implements the standard protocol for the communications media connecting it to host computer 60.

Network 50 can be implemented in a wide range of communications protocols, from FDDI to a simple telecommunications line between two modems. In a network implementation, subsystem 30 provides only the encrypted file; workstation 40 provides the layers of protocol needed for reliable communication on network 50.

Fig. 3 provides more detail of trusted path subsystem 30. Trusted path subsystem 30 consists of a processor 31 connected to a keyboard manager 37, a video manager 38 and cryptographic entity 35. Trusted path subsystem 30 operates in normal mode and in trusted path mode. When in normal mode, workstation trusted path subsystem 30 is transparent to workstation 40. Logical switches 37 and 38 are in the UP position, connecting workstation processor 40 directly to keyboard 20 and display 10. This permits the free transfer of information from keyboard 20 to workstation 40 and from workstation 40 to display 10. In normal mode, workstation processor 40 runs software and communicates with host computer 60 via network 50.

When the user invokes trusted path mode, however, workstation processor 40 is disconnected from keyboard 20 and display 10 by logical switches 37 and 38, respectively. Keyboard 20 and display 10 are then connected to their respective managers in workstation trusted path subsystem 30.

As is shown in Fig. 6, while in trusted path mode, video manager 34 creates a trusted window 82 which is overlaid on the screen display 80 generated by workstation 40 for display 10. Since window 82 is created outside of workstation 40, by trusted elements, it is not possible for malicious software in workstation 40 to control any of the video in trusted window 82. In the preferred embodiment the size of trusted window 82 can vary; if sufficient video RAM is present, window 82 may be as large as the entire display screen.

In a like manner, while in trusted path mode, keyboard manager 36 intercepts keyboard data intended for workstation 40. The data is then routed to cryptographic entity 35, where it is encrypted before being passed over auxiliary port 42 to workstation processing unit 40. Thus, keyboard inputs are protected from eavesdropping and undetected modification until they are decrypted by cryptographic entity 69 on host computer 60.

In one embodiment of the trusted path subsystem of Fig. 3, cryptographic entity 35 uses a pair-wise key to encrypt data to be transmitted from keyboard 20 to host computer 60. At the same time, cryptographic entity 35 decrypts data transmitted from host computer 60 to display 10. The encryption and integrity mechanisms protect the data from eavesdropping and undetected modification as it is passed through workstation processor 40, network 50 and host computer untrusted subsystem 63. Other types of symmetric encryption algorithms such as the Data Encryption Standard (DES) and asymmetric cryptographic techniques such as public key can also be used. Furthermore, the encryption algorithm can either be implemented in software, programmable hardware, or custom hardware.

Trusted path mode can be invoked in a number of ways. In one embodiment, a switch on trusted path subsystem 30 can be used to manually activate trusted path mode. A second method would be to invoke trusted path mode by a combination of keys pressed simultaneously on keyboard 20 (like the control/alt/delete key sequence on a PC-compatible computer). A third embodiment would require that the user insert some sort of token device into subsystem 30. A token device might range from a smart card to a cryptoignition key. In the preferred embodiment, subsystem 30 would also have a feedback mechanism such

as a light to notify the user that subsystem 30 was in trusted path mode.

The trusted path mode, used in conjunction with cryptographic entity 69 on host computer 60, provides security services such as user authentication, data confidentiality, data integrity and data origin authentication and confinement of malicious software. The user is authenticated to trusted path subsystem 30 and this authentication is securely passed to trusted subsystem 67 in MLS computer 60. Data passed between cryptographic entities 35 and 69 is protected from unauthorized disclosure and undetected modification. Cryptographic entities 35 and 69 also assure that the data was sent from one cryptographic entity to its peer cryptographic device. In addition, malicious software on workstation 40, network 50 or untrusted subsystem 63 is confined so that it cannot dupe the user or trusted subsystem 67 into performing an insecure action.

The user can be authenticated to the trusted computing system by either authenticating himself directly to trusted path subsystem 30 or by going through subsystem 30 to host computer 60. In the first method, the user can authenticate himself to subsystem 30 via such means as a personal identification number (PIN), a password, biometrics or a token device such as a smart card or a cryptographic ignition key. Once the user has authenticated himself to subsystem 30, subsystem 30 relays the authentication to trusted subsystem 65. The step of relaying authentication can be done by either automatically entering trusted path mode as part of the authentication process or by having subsystem 30 relay the authentication data at a later time.

A second method for authenticating a user would be to first enter trusted path mode and then authenticate the user directly to host computer 60.

This approach would reduce the processing power needed on subsystem 30.

In its simplest form, trusted path subsystem 30, in conjunction with workstation 40, display 10 and keyboard 20, forms an assured terminal. Data typed on keyboard 20 or extracted from a pointing device such as a mouse is encrypted and transferred over network 50 to host computer 60. Screen display data transferred from host computer 60 is decrypted and displayed within trusted window 82. Such a terminal might be implemented as a relatively dumb terminal such as a VT100, or it could be implemented as a X Windows terminal. The X Window embodiment would be useful since it would allow the creation of multiple trusted windows 82 and would permit the assigning of a different security level to each window. Such a mechanism would permit qualified users to cut information from a document of one sensitivity and paste it into a document of a different sensitivity.

An assured terminal is especially useful in an environment where you are trying to maintain a number of security levels despite having a workstation which will only operate at one level. An example is a trusted computing system mixing single level secure workstations with a multi-level computer with three security levels: unclassified (least sensitive), secret (much more sensitive), and top secret (most sensitive). Trusted path subsystem 30 can be used to expand the capabilities of the single level workstation since subsystem 30 allows the user to essentially disable subsystem 30, do all his work at the level permitted by the workstation (say, secret) using all the capabilities of his workstation and whatever facilities are available on the multilevel computer. Then, if the user has a small amount of work that he or she needs to do at top secret, the user can invoke trusted mode in subsystem 30, isolate their workstation, its processor memory and

storage devices, and he has, in effect, a keyboard and a terminal connected to a secure communications device through a multilevel host. The user can then do the operations required at top secret.

The cryptographic techniques applied in subsystem 30 will ensure that none of the top secret information going to or from the multilevel secure computer is linked to files within workstation 40 or is captured and copied on the network.

Likewise, if a user had to do a small amount of unclassified work, he could put the workstation into trusted path mode using subsystem 30. The user could, through a trusted path, invoke an unclassified level and again the cryptographic techniques applied at each end of the link would prevent secret information from being mixed in with the unclassified information. The system essentially provides a pipe to keep data from one security level from being mixed into data at a different security level.

Trusted subsystem 30 is not, however, limited to a role as an assured terminal. In a file server application, files stored at host computer 60 or within workstation 40 could be transferred to subsystem 30 for data processing tasks such as editing, reviewing the file or transferring it as electronic mail. In a client server application, processor 31 could execute one or more client processes such as an editor or a communications process. Software and firmware which could be implemented inside trusted path subsystem 30 would be limited only by the amount of storage within subsystem 30 and the review and approval process required to provide clean software.

Trusted path subsystem 30 has access not only to files on host computer 60 but also on workstation 40. Files transferred from either computer 60 or workstation 40 can be manipulated and transferred to other computers or workstations. For example, a secure electronic mail

system could be implemented in which trusted path subsystem 30 is used for reviewing, reclassifying, and electronically signing messages. A document file from computer 60 or workstation 40 can be displayed and reviewed. If appropriate, the user may downgrade its sensitivity level by attaching a different security level to the document. The finished file can then be sent via electronic mail to other users.

In one embodiment of such an electronic mail function, subsystem 30 would go out on the network to the directory server to retrieve the names, electronic mail addresses and public key information of the intended recipients. The directory server could be implemented as either a trusted or an untrusted process on host computer 60 or on another network computer. Subsystem 30 would then attach the addresses to the file, affix a digital signature, encrypt the final product and send it through host computer 60 to the designated addresses.

In another embodiment of such a function, in a system without a MLS computer, secure electronic mail is possible by first establishing a trusted path from the user to processor 31. The user then accesses files of workstation 40 (or on other network computers), displays and reviews the file, accesses an unsecured directory server to retrieve the names, electronic mail addresses and public key information and sends the encrypted message via electronic mail to its recipient.

Processor 31 can also be used to control video manager 34 in order to implement and control the user interface. Such an approach would permit the use of a graphical user interface (GUI) within trusted window 82 that would reduce the amount of screen information transferred by host computer 60. This approach also permits the user to implement, through processor 31, multiple trusted windows 82 at the user node in order to perform the cut-and-paste function referred to above.

In the preferred embodiment, subsystem 30 is a modular design in which processor 31 and cryptographic entity 35 are kept constant and video manager 34 and keyboard manager 36 are designed so that they can be replaced easily to handle different displays and keyboards. In one embodiment, subsystem 30 is designed to be portable. A portable subsystem 30 can be used to turn any modem equipped computer with the requisite auxiliary data port into a secure data terminal or computer.

Fig. 4 is a block diagram representation of an alternate embodiment of trusted path subsystem 30. In Fig. 4, processor 31 is connected through network interface 39 to network 50 and through communication port 48 to workstation 40. In the embodiment shown in Fig. 4, workstation processing unit 40 is isolated from the network. This approach allows the encryption of all network traffic associated with the user node. In the embodiment shown in Fig. 4, communication port 48 can be a communication medium ranging from RS0232 to an unsecured Ethernet.

A more detailed representation of one embodiment of trusted path subsystem 30 is shown in Fig. 5. In Fig. 5, keyboard logical switch 37 receives data from keyboard 20 and routes it to processor 31. During normal mode, processor 31 then sends the received keyboard data directly over keyboard port 46 to workstation 40.

In contrast, in trusted path mode, processor 31 captures the received keyboard data and sends it to cryptographic entity 35 for encrypting. No information is sent over keyboard port 46 to workstation 40. The resulting encrypted keyboard data is instead sent through auxiliary data port 42 to workstation 40 and from there to computer 60.

Video data from workstation 40 is transmitted from video port 44 to video manager 34. During normal

mode, the video data is sent through to display 10 without modification. During trusted path mode, however, the video data transferred from video port 44 is overlaid, at least in some part, by video data generated by video manager 34.

A representative video manager 34 is shown generally in Fig. 5. Video manager 34 consists of video synchronization hardware 72, video RAM 74, video driver 78 and video multiplexer 76. Video synchronization hardware 72 receives synchronization signals from video port 44 and uses the signals to coordinate the display of data from video RAM 74 with the display generated by workstation 40. During normal mode data from video RAM 74 is not used; video is transferred directly from workstation 40 through video multiplexer 76 to display 10. When, however, trusted path subsystem 30 is placed into trusted path mode, video data stored in video RAM 74 is used instead of the normal video stream to create trusted window 82.

In one embodiment synchronization hardware 72 uses the synchronization signals received from workstation 40 to control the reading of data from video RAM 74 and the conversion of that data into a video signal by video driver 78. The output of video driver 78 is then used to drive video multiplexer 76. Synchronization hardware 72 controls video multiplexer 76 in order to switch between the video generated by workstation 40 and the video being read from video RAM 74. The output of video multiplexer 76 is driven through video amplifiers to display 10.

The design of the video hardware needed to overlay one display on top of another is well known in the art. Window 82 can be synched up to the video going to display 10. Typically, if window 82 is not full screen, video synchronization hardware 72 counts the number of lines to the first line of window 82, counts in the number of pixels, and inserts the video at that

point. Trusted path video data is then written for the desired number of pixels and video multiplexer 76 is switched back to normal video for the remainder of the video line. This mechanism provides flexibility in placement and sizing of window 82 on screen 80.

Video multiplexer 76 can be built using a crosspoint video switch such as the MAX456 manufactured by Maxim Integrated Products. Video data to and from the crosspoint video switch can be buffered using the MAX457 by Maxim Integrated Products. Video RAM 74 can be any commercial video RAM. A typical video RAM is the MT42C8256 manufactured by Micron Technologies Inc. It should be obvious that the given design can be easily adapted for either a color or a black and white display or even for a black and white overlay of a color display.

In one embodiment, host computer 60 transmits, as encrypted packets, video data to be displayed within trusted window 82. The encrypted packets are passed to processor 31 by workstation 40 and then on to encryption device 35. Encryption entity 35 decrypts the video data and places it into video RAM 74. Synchronization hardware 72 then activates video multiplexer 76 and video RAM 74 in order to display the decrypted secure video data.

In a second embodiment (not shown), processor 31 creates the video overlay data and writes that data to video RAM 74. Display of the data is as above.

A trusted computing system based on unsecured, commercially available, workstations, trusted path subsystems and multilevel secure computers provides a powerful, highly secure computing environment. The ability of such a system to compensate for unsecured workstations allows the designers of such systems to use the latest versions of commercially available hardware and software without compromising the security of the system.

For instance, a user of a workstation may wish to edit a secret document and reclassify the edited document as unclassified. The document can be loaded into the workstation, edited with the user's favorite word processing software package, and saved. Then, in order to classify the document as unclassified, the user would invoke trusted path mode, the trusted window would be displayed and the user could review the revised document to verify that no additional information had been attached to the file. The reviewed document could then be released as an unclassified document and the user would then returns to normal mode.

The unique placement of cryptographic entity 35 relative to workstation 40 allows a single workstation to be used at different levels of security sensitivity. Therefore, instead of systems in which a workstation is required for each level of security sensitivity, in the present system a single commercial workstation may be used to protect and access a range of security levels.

Finally, the end-to-end characteristic of the encryption permits secure communication without the need to perform costly analysis of complex elements such as network controllers. The invention also allows use of commercial off-the-shelf workstations and network components and can be used with a variety of keyboards and displays.

Although the present invention has been described with reference to the preferred embodiments, those skilled in the art will recognize that changes may be made in form and detail without departing from the spirit and scope of the invention.

What is claimed is:

1. A secure computing network, comprising:

a network computer, wherein the computer comprises

a trusted subsystem; and

encryption means for encrypting and decrypting data transferred to and from the trusted subsystem;

communications means, connected to the network computer, for permitting data transfer between the network computer and other computers;

an input/output device;

a workstation comprising:

first communications interface means, connected to the communications means, for transferring data between the workstation and the network computer;

input/output device interface means for transferring data between the workstation and the input/output device; and

second communications means for transferring data between the workstation and another processor; and

trusted path means, inserted between the input/output device and the input/output device interface means and connected to the second communications means, for intercepting data transfers between the input/output device interface means and the input/output device, wherein the trusted path means comprises encryption means for encrypting and decrypting the data transfers and for routing such transfers over the second communications means to the trusted subsystem.

2. The secure computing network of claim 1 wherein the network computer is a multilevel secure computer capable of recognizing data of varying sensitivity and users of varying authorizations.

3. The secure computing network of claim 1 wherein the input/output device comprises a keyboard.

4. The secure computing network of claim 1 wherein the input/output device comprises a display device.

5. The secure computing network of claim 1 wherein the input/output device comprises a pointing device.

6. A secure computing network, comprising:

a network computer, wherein the computer comprises

a trusted subsystem; and

encryption means for encrypting and decrypting data transferred to and from the trusted subsystem;

communications means, connected to the network computer, for permitting data transfer between the network computer and other computers;

an input/output device;

a workstation comprising:

input/output device interface means for transferring data between the workstation and the input/output device; and

workstation communications means for transferring data between the workstation and another processor; and

trusted path means, inserted between the input/output device and the input/output device interface means and connected to the workstation communications means, for intercepting data transfers between the input/output device interface means and the input/output device, wherein the trusted path means comprises encryption means for encrypting and decrypting the data transfers and network interface means, connected to the communication means, for transferring

the encrypted data transfers between the trusted path means and the trusted subsystem.

7. The secure computing network of claim 6 wherein the network computer is a multilevel secure computer capable of recognizing data of varying sensitivity and users of varying authorizations.

8. The secure computing network of claim 6 wherein the input/output device comprises a keyboard.

9. The secure computing network of claim 6 wherein the input/output device comprises a display device.

10. The secure computing network of claim 6 wherein the input/output device comprises a pointing device.

11. A trusted path subsystem capable of being connected between an input/output device and a processor of a workstation in order to provide secure communication with a multilevel secure computer network server, the subsystem comprising:

input/output manager means for selectively intercepting, under user control, data transferred from the input/output device to the processor and from the processor to the input/output device;

encryption means for encrypting the intercepted data before transferring the encrypted data to the processor; and

decryption means for decrypting the intercepted data before transferring the decrypted data to the input/output device.

12. The trusted path subsystem according to claim 11 wherein the input/output manager means comprises keyboard manager logic, wherein the keyboard manager logic comprises:

a keyboard interface which captures information generated by a keyboard; and

processing means for transferring the captured information to a workstation processor, wherein the processing means transfers the captured information on a first path when in a first mode and on a second path when in a second mode.

13. The trusted path subsystem according to claim 11 wherein the input/output manager means comprises a video manager which can be used to generate a trusted window overlay on a video screen, wherein the video manager comprises:

a video multiplexer having first and second input ports and an output port, wherein the first input port can be connected to an external video signal and wherein the output port can be connected to a video display;

a video data memory;

converter means, connected to the video data memory and the second multiplexer input port, for converting data read from the video data memory into a trusted video signal representative of that data and for applying the trusted video signal to the second video multiplexer input port; and

video synchronization means, connected to the video data memory and the video multiplexer, for controlling the video data memory and the video multiplexer so as to insert the trusted video signal into the video signal generated at the video multiplexer output port.

14. A method of securely transferring data in a network comprising an unsecured workstation connected to a multilevel secure computer server, wherein the workstation comprises a processor and an input/output device and wherein the multilevel secure server comprises a trusted subsystem and encryption means for encrypting and decrypting data transferred to and from

the trusted subsystem, the method comprising the steps of:

providing trusted path means for providing a user selectable secure communications path between the input/output device and the trusted subsystem; and

inserting the trusted path means between the input/output device and the processor.

15. A method for providing secure file transfer capability on an unsecured workstation connected over a network to a second computer, wherein the workstation comprises a workstation processor and an input/output device and wherein the second computer comprises a trusted subsystem and encryption means for encrypting and decrypting data transferred to and from the trusted subsystem, the method comprising the steps of:

providing means for creating a trusted path between the input/output device and a trusted subsystem, said trusted path means including a trusted processor capable of executing a secure electronic mail program;

inserting the trusted path means between the input/output device and the workstation processor;

downloading from the workstation processor to the trusted processor a file to be transferred to the second computer;

displaying, on the input/output device, a representation of the file to be transferred;

if the file is as expected, transferring the file to the second computer; and

if the file is not as expected, generating an error message.

16. The method according to claim 15 wherein the step of generating an error includes allowing secured processing on the file.

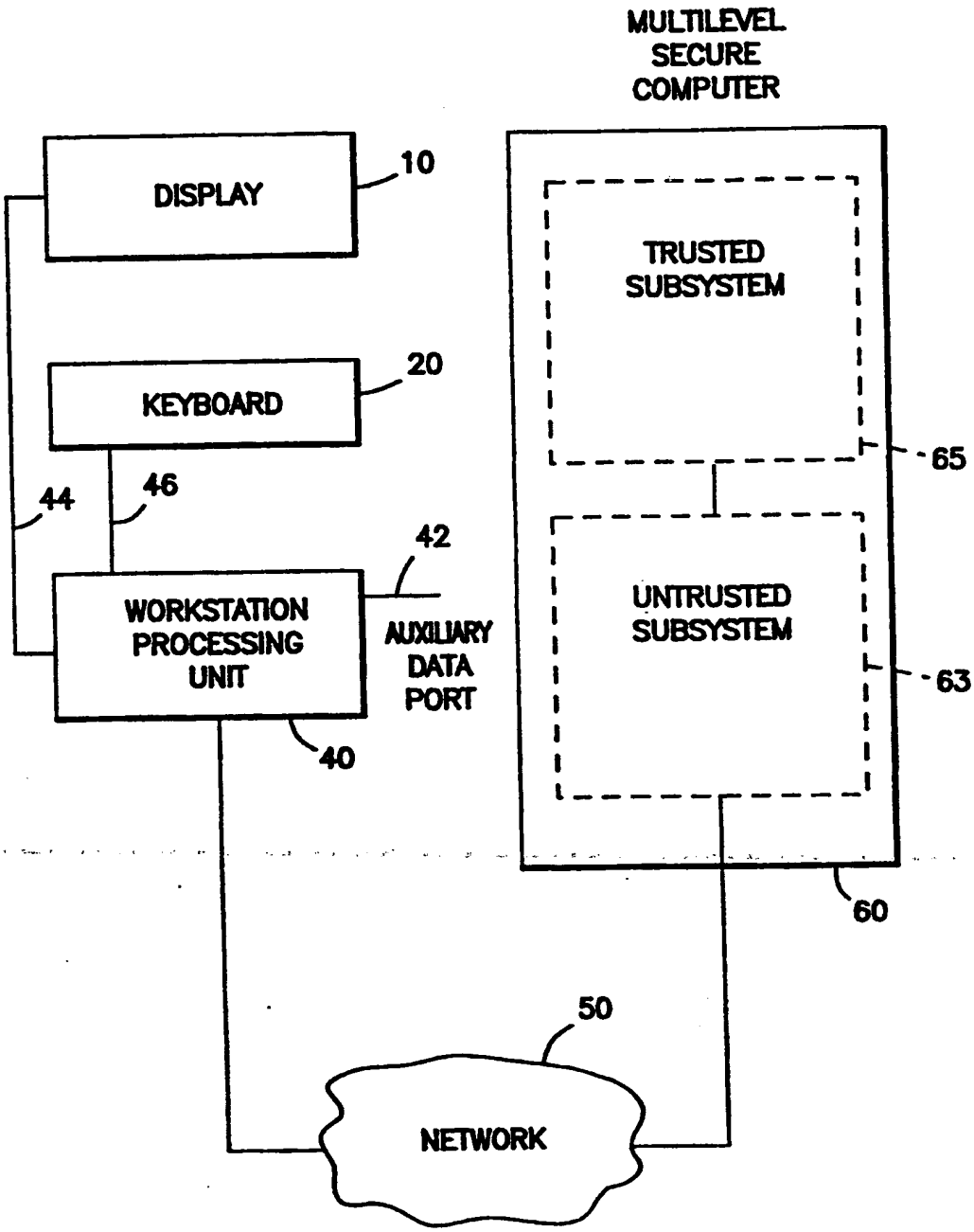


FIG. 1

PRIOR ART

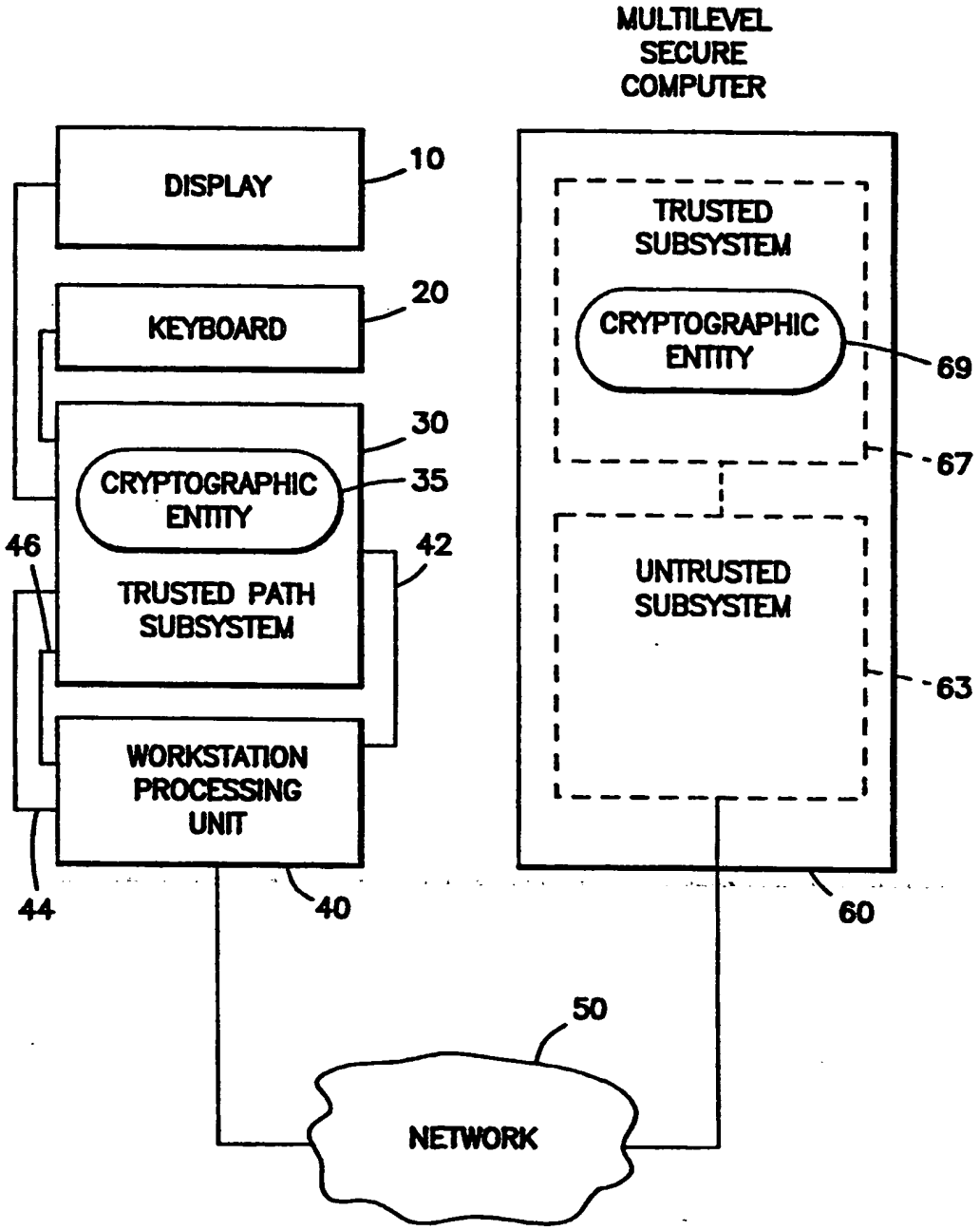

MULTILEVEL SECURE COMPUTER
DISPLAY
10
KEYBOARD
20
CRYPTOGRAPHIC ENTITY
30
35
TRUSTED PATH SUBSYSTEM
46
42
WORKSTATION PROCESSING UNIT
44
40
TRUSTED SUBSYSTEM
CRYPTOGRAPHIC ENTITY
69
67
UNTRUSTED SUBSYSTEM
63
60
50
NETWORK

FIG. 2

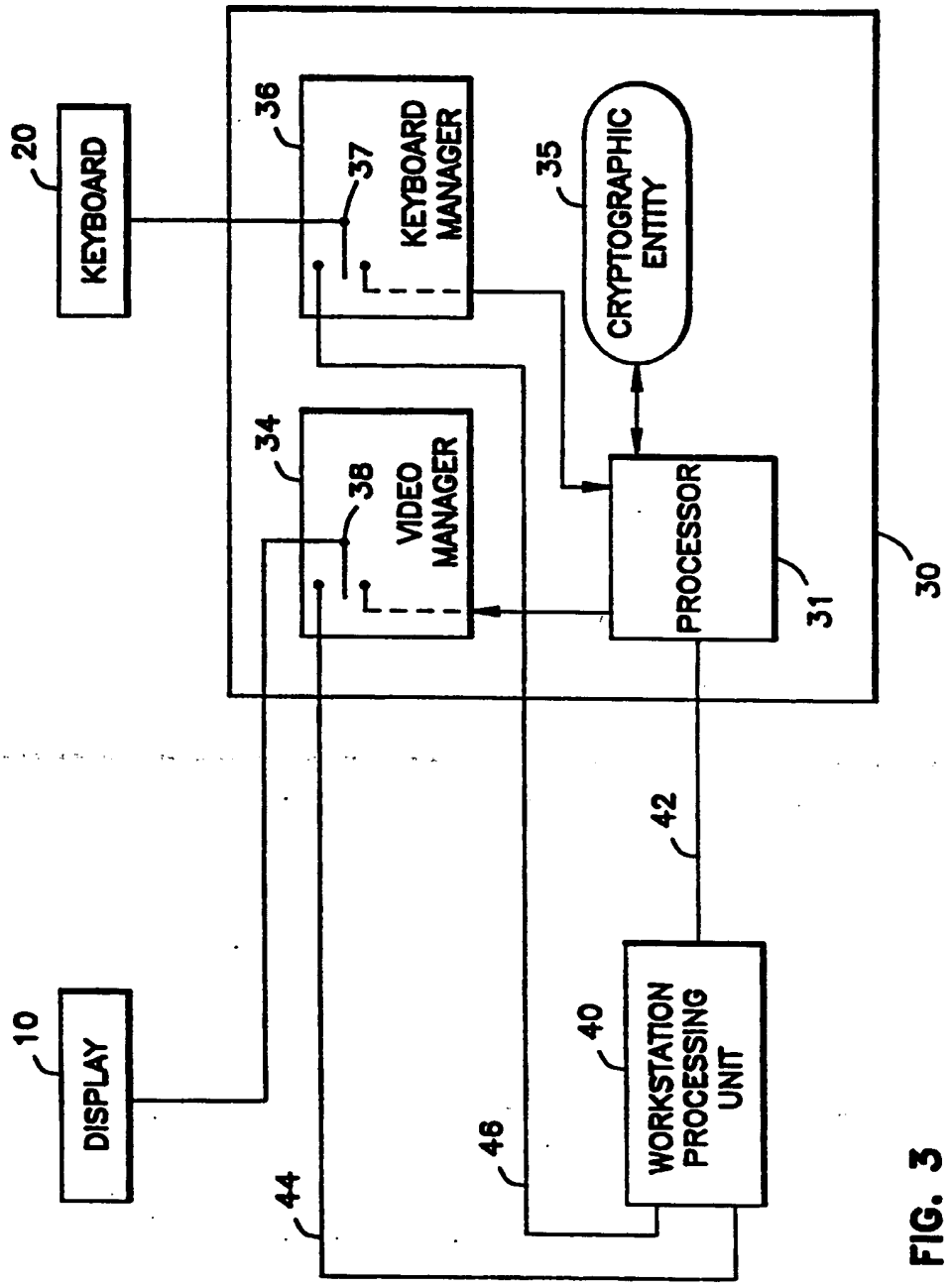

20
KEYBOARD
36
37
KEYBOARD MANAGER
35
CRYPTOGRAPHIC ENTITY
34
38
VIDEO MANAGER
PROCESSOR
31
30
42
10
DISPLAY
40
WORKSTATION PROCESSING UNIT
46
44

FIG. 3

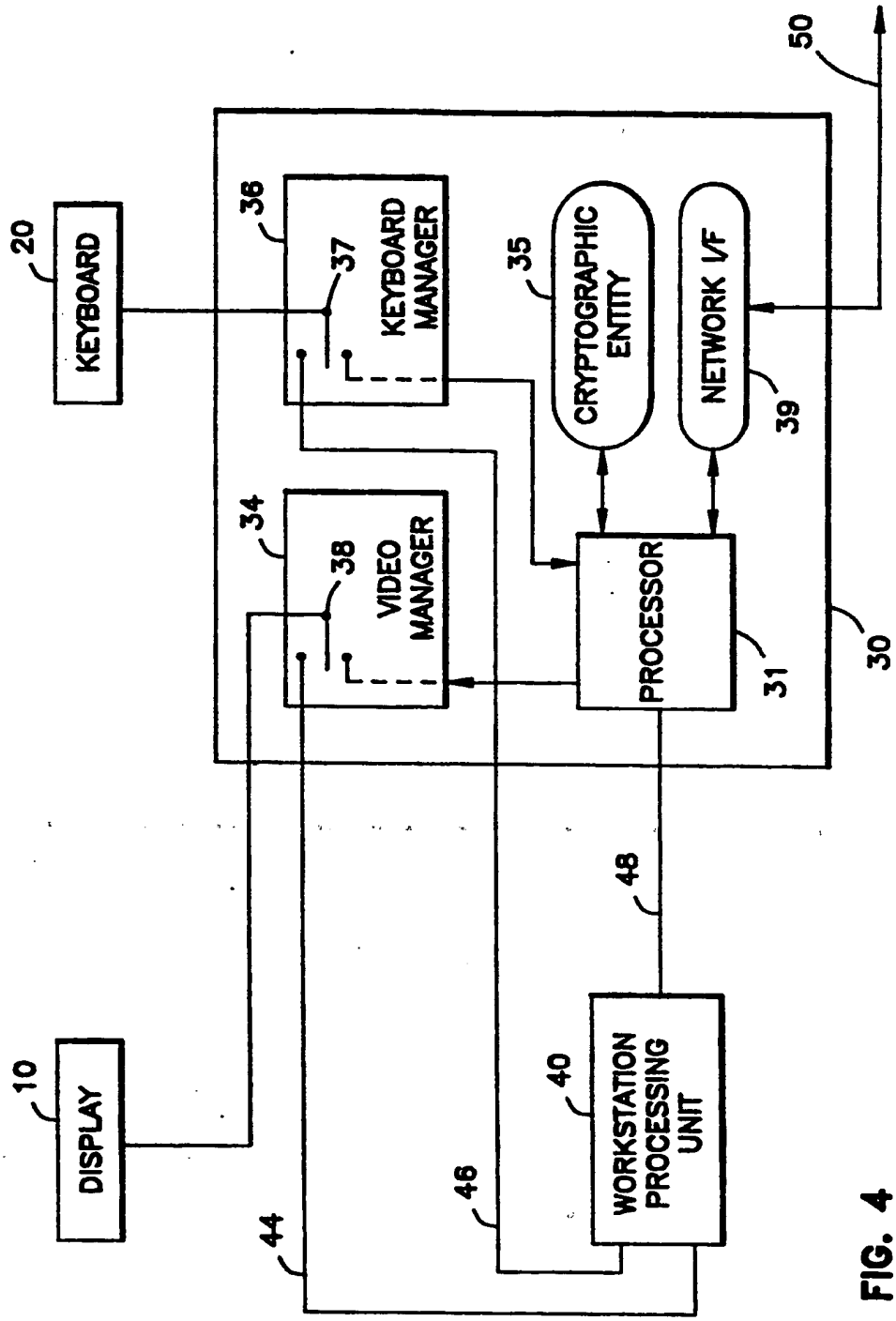

50
20
KEYBOARD
36
37
KEYBOARD MANAGER
35
CRYPTOGRAPHIC ENTITY
NETWORK I/F
39
34
38
VIDEO MANAGER
PROCESSOR
31
30
48
10
DISPLAY
40
WORKSTATION PROCESSING UNIT
46
44

FIG. 4

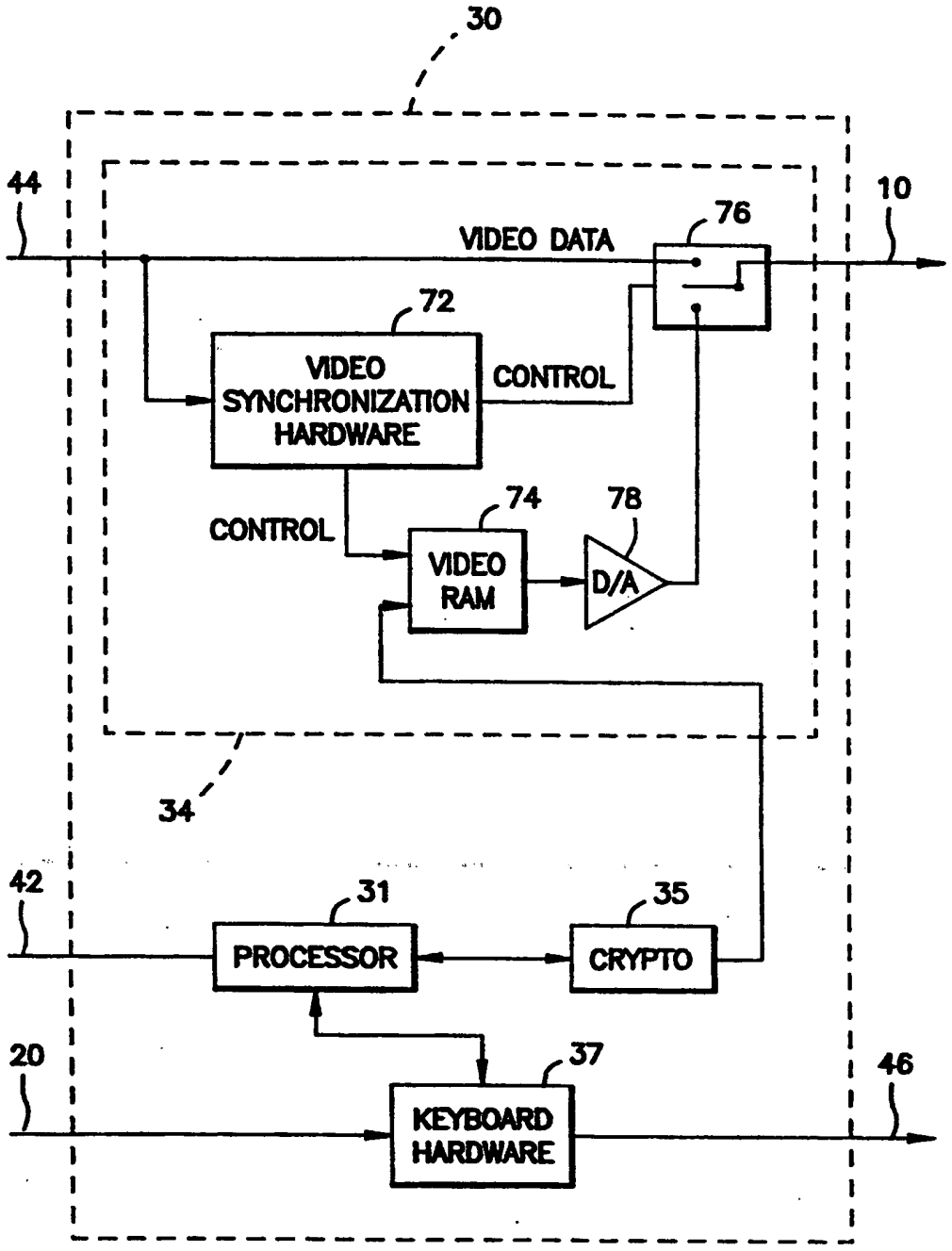

30
44
10
VIDEO DATA
76
72
VIDEO SYNCHRONIZATION HARDWARE
CONTROL
CONTROL
74
78
VIDEO RAM
D/A
34
42
31
35
PROCESSOR
CRYPTO
20
37
46
KEYBOARD HARDWARE

FIG. 5

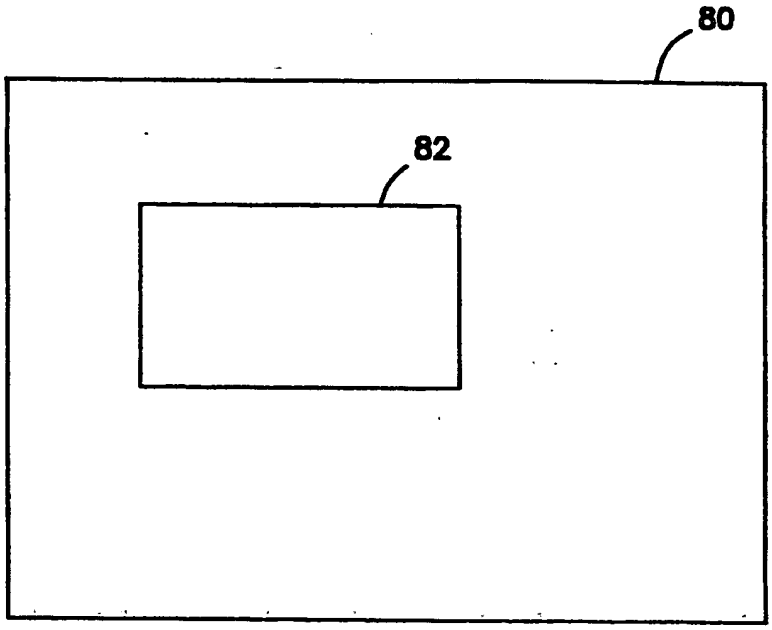


FIG. 6

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 93/06511

A. CLASSIFICATION OF SUBJECT MATTER
IPC 5 G06F12/14 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 5 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
11 Y	EP,A,0 192 243 (HONEYWELL) 27 August 1986 cited in the application see abstract; figures 3,4 see page 18, line 16 - page 21, line 14 see claims 1-10	1-16
11 P,Y	WO,A,92 17958 (SECURE COMPUTING TECHNOLOGY) 15 October 1992 cited in the application see abstract; figure 1 see page 3, line 35 - page 6, line 16 see page 7, line 22 - page 10, line 35	1-16

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
23 November 1993	07. 12. 93

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	POWELL, D

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	IEEE SYMPOSIUM ON SECURITY AND PRIVACY, 4 May 1992 , OAKLAND, US; pages 226 - 239 J.EPSTEIN ET AL 'Evolution of a Trusted B3 Window Prototype' see figure 3 see page 229, left column, line 1 - page 230, right column, line 5 see page 231, right column, line 23 - page 232, left column, line 32 see page 233, left column, line 5 - page 234, left column, line 15 ---	3-5,8-13
Y	PROC. FALL JOINT COMPUTER CONF., 25 October 1987 , DALLAS, US; pages 411 - 420 J.PICCIOTTO ET AL 'Privileges and Their Use by Trusted Applications' see page 415, left column, line 23 - page 419, left column, line 18 ---	15,16
A	EP,A,0 096 628 (DIGITAL EQUIPMENT CORPORATION) 21 December 1983 see abstract; figure 1 ---	13
A	EP,A,0 443 423 (DIGITAL EQUIPMENT CORPORATION) 28 August 1991 see abstract; figures 4A,4B -----	15,16

INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No
PCT/US 93/06511

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A-0192243	27-08-86	US-A-	4713753	15-12-87
		CA-A-	1252907	18-04-89
		JP-A-	61195443	29-08-86
WO-A-9217958	15-10-92	AU-A-	1576792	02-11-92
EP-A-0096628	21-12-83	US-A-	4498098	05-02-85
		AU-A-	1501683	08-12-83
		CA-A-	1185377	09-04-85
		JP-C-	1628356	20-12-91
		JP-B-	2052911	15-11-90
		JP-A-	59057279	02-04-84
EP-A-0443423	28-08-91	AU-A-	7103191	15-08-91